Abstract

Purchase of information items from a merchant over the Internet or other network is implemented so as to ensure that the merchant is unable to identify the particular information item(s) purchased by a user. The user when considering purchase of a given information item is permitted to access a corresponding signed ciphertext of that item. The signed ciphertext in an illustrative embodiment includes a first ciphertext portion in the form of a symmetric key encrypted using a public key associated with the merchant, a second ciphertext portion corresponding to the information item encrypted using the symmetric key, an unencrypted description of the information item, and a tag corresponding to a signature. The user requests purchase of the information item by sending a blinded version of the first ciphertext portion to a payment server along with an appropriate payment. The payment server decrypts the blinded version of the first ciphertext portion and returns the resulting symmetric key to the user. The user then utilizes the symmetric key to decrypt the second ciphertext portion so as to obtain the desired information item. The decrypting operation performed by the payment server may be implemented using at least part of a set of multiple rounds, with the user providing a blinded ciphertext and receiving a corresponding decryption result for each of the rounds.